

2024

**Making the connected world
a safer and smarter place**

Sustainability report



Contents

A word from our CEO	3
This is AddSecure	4
Secure IoT solutions back UN SDGs	6
An expanding portfolio of solutions	7
Sustainability statement	11
General information	12
Our strategy	13
Our business model – how we create value	15
Stakeholder dialogue and engagement	17
Material impacts, risks and opportunities	19
Governance	23
Sustainability framework	25
Environmental information	26
Climate change and carbon emissions	26
AddSecure’s climate transition plan	28
2024 performance	30
Resource use and circular economy	32
Social information	34
Workforce	34
Customers and end-users	37
Workers in the value chain	39
Governance information	41
Business conduct	41

We live in an increasingly connected world where IoT and data have the potential to reshape the way we produce, consume and live. As sensor-based and internet-connected devices multiply, they will handle even more life- and business-critical applications. This makes it more important than ever to handle data and communications in a secure way. AddSecure offers secure IoT connectivity and end-to-end solutions, helping customers optimise operations, drive business and uphold vital societal functions. This way, we help transform society and make the connected world a safer and smarter place.

.....

About this report
This is AddSecure’s fifth sustainability report. The purpose of the report is to present how we create value and contribute to a safer and smarter world through our secure IoT solutions. Additionally, the report informs and reports on AddSecure’s 2024 objectives and progress within our strategic focus areas. The report is inspired by global standards for sustainability reporting, including the European Sustainability Reporting Standards (ESRS) and the GRI Standards.

Contact
Johanna Giorgi
Chief Sustainability Officer
johanna.giorgi@addsecure.com

Boiling it down to trust, value and teams

Global challenges such as economic volatility, climate change, and geopolitical tensions underscore the need for resilient and adaptive solutions. IoT plays a pivotal role in addressing these challenges. From smart buildings and connected healthcare to industrial automation and intelligent transportation systems, IoT is enhancing efficiency, improving safety, and creating unprecedented opportunities for innovation.

We have made it our business to provide secure IoT solutions that help create a smarter and safer world. As a rapidly growing company within the realm of IoT, we are used to having to adapt to technological, regulatory and market changes all while adding new entities, solutions, geographies and people to our group. That things will change is, in fact, one of few things that one working with AddSecure can be certain of.

To navigate a world marked by uncertainties, having a strong internal compass is more crucial than ever. At AddSecure, we pilot along three strategic objectives that we see as key to ensure our continued growth and to manage our most material impacts, risks and opportunities:

- 1. Building trust in our solutions** is paramount. We are committed to safeguarding data and ensuring the highest standards of security to protect our customers and their information.
- 2. Delivering value to customers** We strive to understand their needs and deliver solutions that provide tangible value and drive their success.

- 3. Forming strong and dedicated teams** Our people are our greatest asset. By fostering a culture of collaboration, engagement, and continuous learning, we empower our teams to excel and achieve their full potential.

As we close the books on 2024, I am filled with immense pride. Proud of supporting more than 70,000 customers reap the benefits of secure IoT. Proud of having grown our portfolio and presence by welcoming three new organisations to the AddSecure Group. Proud of receiving recognitions both for our solutions, our way of working and our workplace. Proud of being well underway to achieving a group-wide ISO27001 certification. And, of course, immensely proud of all our co-workers who made this happen. Our success is a testament to the dedication and resourcefulness of our team.

Looking ahead, we are excited about the possibilities that lie before us. The IoT landscape is evolving at an unprecedented pace, and we are well-positioned to capitalise on the opportunities it presents. We will continue to innovate, collaborate, and push boundaries, always with the goal of delivering value to our customers and stakeholders.

Imagination is our only limit.

Stockholm May 2025
Stefan Albertsson, CEO



2024 highlights

- We continued to broaden our portfolio through the acquisitions of Connecting Solutions and Astrata Europe, and by expanding into the UK alarm signalling market through our collaboration agreement with BT Redcare.
- We increased the number of SIM cards connected through our connectivity platform, Link with 24%, making the connected world a safer place.
- We received the 2024 Europe Market Leadership Award by Frost & Sullivan, and the Connected Vehicle Award by German Telematik Markt.
- We kept our EcoVadis sustainability gold rating, placing us in the top 5 percent of the more than 130,000 companies rated globally.
- We expanded the scope of our ISO 27001 certification to all corporate functions and the entire Smart Alarms business unit's operations across Europe – going for full coverage 2025!
- We were recognised as one of the top 25 winners of the Inspiring Workplaces Europe 2024 award.

TOP RANKED AND CERTIFIED SUSTAINABILITY PROGRAM



This is AddSecure

AddSecure is a leading European provider of secure IoT connectivity and end-to-end solutions. We help customers optimise their operations and drive business value. Our solutions are used within the areas of buildings, alarms, transportation, personal safety, elderly care, construction, power grids, waste management – and more.

We are a fast-growing company with an ambition to create a safer and smarter world. Sustainability guides us in our daily operations as well as in our innovation and growth strategies. Sustainability inspires us to create profitable smart business in new ways and by new means.

Majority owned by **Castik Capital** since 2019

1,000+

Employees (end of 2024)

70k

Customers¹

713k

Managed SIM connections

€220M

Annual revenue (2024)

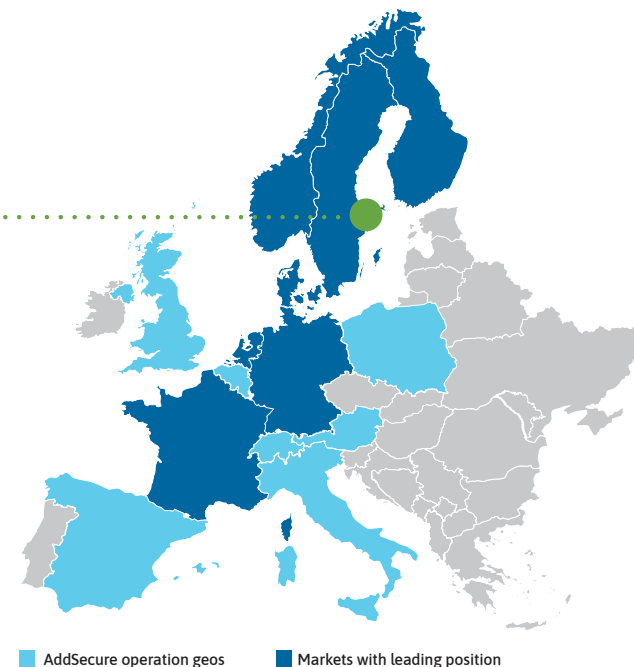
73%

Recurring revenue

14

Silent heroes nominated and awarded by our employees since 2023²

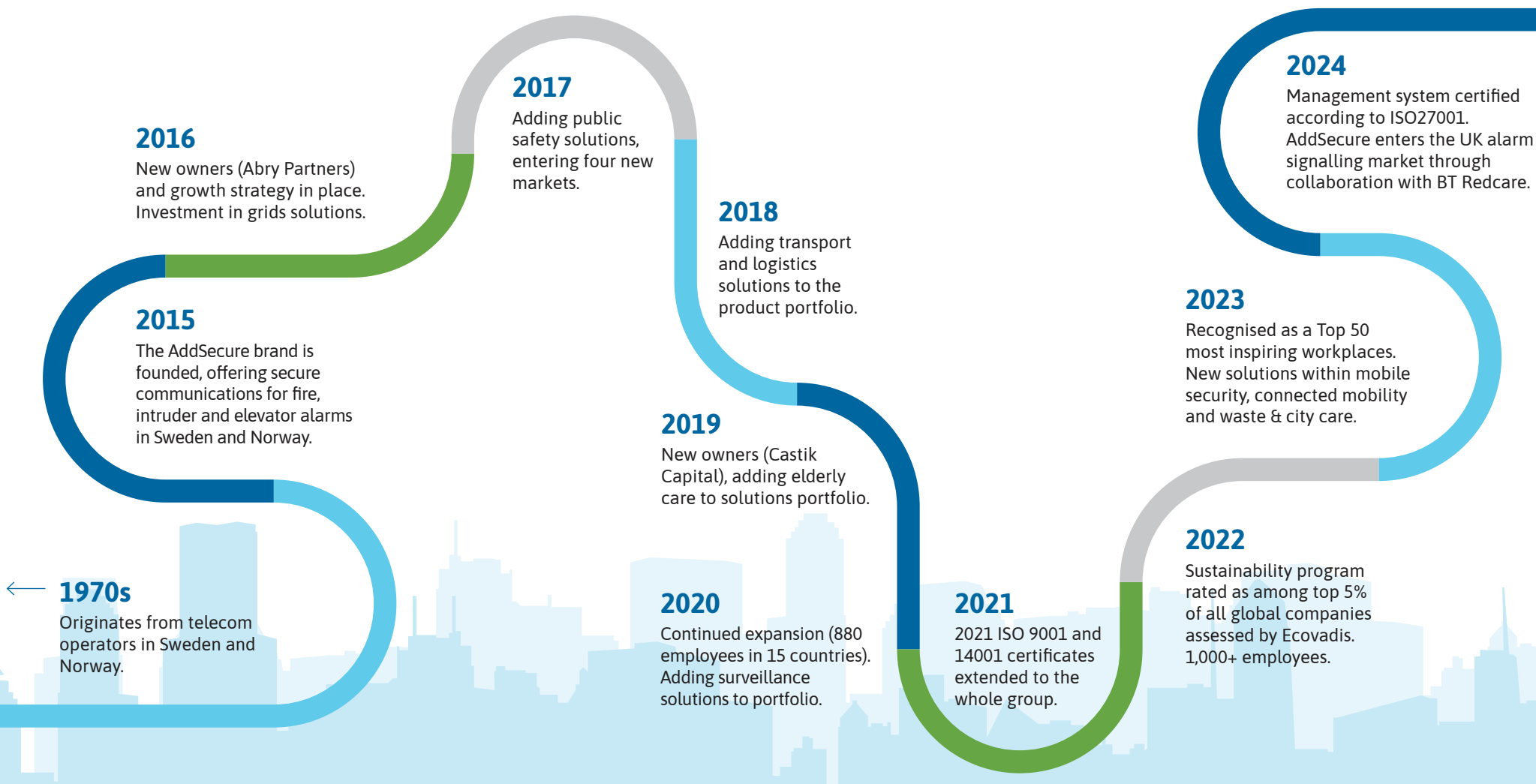
Headquarters in
Stockholm, Sweden



¹ Based on billed entities, including partners who account for multiple end-users.

² Silent Hero award acknowledges co-workers that live our core values and significantly contribute to the team spirit.

Our journey



Secure IoT solutions back UN SDGs

According to the World Economic Forum, 70% of the UN Agenda 2030 and its 169 targets can be directly supported by technology applications, where IoT plays a role in 33% of the technological applications mapped.¹ Data will continue to have a transformational impact on economies and societies, seeing benefits in every single aspect of our lives, ranging from more conscious energy consumption and product, material, and food traceability, to healthier lives and better healthcare. As sensor-based and internet-connected devices multiply, they will handle even more societal, life- and business-critical applications. This makes it more important than ever to handle data and communications in a secure way.

Our secure IoT solutions used within public safety, rescue services, building security and automation, elderly care, transport and logistics, construction, utilities, smart cities, and more, are all contributing to the United Nations' Sustainable Development Goals (SDGs). By offering secure IoT solutions end-to-end, we help reshape the way we produce, consume and live in a connected world. Our secure IoT solutions provide deep customer value by solving complex needs, provide quick responses to events, and improve operational efficiency and productivity.

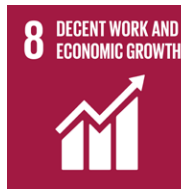
AddSecure's secure IoT solutions actively contribute to the UN sustainable development goals.



Smart homecare, monitoring and wearables give access to health-care services that combine human care with reliable and safe technology.



IoT solutions for remote monitoring and configuration help secure water supply and guarantee water quality.



Remote monitoring and management enable end-users to improve their resource efficiency and create safe working environments.



Connected sensor-based grid, building and mobility management systems help minimise pollution, emissions, and energy consumption.



IoT solutions for remote monitoring and management of transports, buildings and grids help optimise use of energy and resources.



Right information to the right people at the right time helps provide safe, nonviolent, inclusive and effective learning environments for all.



Smart grid solutions help expand infrastructure and upgrade technology for modern and sustainable energy services for all.



IoT enabled tracking devices help optimise transports of goods and lower emissions.



IoT solutions help monitor and optimise logistics and distributions networks, optimising use of resources and reducing emissions and waste.



Using secure data and secure critical communications help prevent and respond to alarms, threats and emergencies.

¹ World Economic Forum, "Unlocking Technology for the Global Goals" http://www3.weforum.org/docs/Unlocking_Technology_for_the_Global_Goals.pdf

An expanding portfolio of solutions





CASE: Waste and City Care

Waste management system

Effective placement of public waste bins is crucial to combat littering. Properly positioned bins encourage people to dispose of trash correctly, reducing litter in public spaces and nature. Digitised containers, equipped with sensors, provide real-time data on fill levels and usage patterns, enabling timely emptying, reducing littering risks and making it possible to plan collections more efficiently, reducing costs and CO₂ emissions. Data analysis helps optimise bin placement based on actual needs, ensuring bins are available where most needed. In addition, the data from the BMS (Bin Management System) can be used to inform the public about where waste bins are available and the importance of disposing of waste properly.



CASE: Transport Management



Improved efficiency for Aldi

Aldi lacked standardised processes across its pan-European operations, with no data on fuel consumption and only paper-based temperature records. Legal requirements were handled manually across different regions, resulting in inefficiencies. Aiming for automation and cost reductions, AddSecure supported Aldi by implementing solutions across eight countries, including ~250k telematics units connecting +1,000 trailers and 60 distribution centres. As a result, Aldi improved operational efficiency and reduced its fuel consumption by 7%.



CASE: School Safety

AddSecure's school safety report

Ensuring the safety of students and staff in schools is a top priority. According to AddSecure's "Trygg skola 2024" report, there is a growing concern among parents and educators about the increasing incidents of threats and violence in schools.

The report highlights that over half of the parents worry about the lack of resources affecting school safety. Incidents of threats and violence have doubled over the past decade, emphasising the need for effective safety measures.



AddSecure offers a comprehensive school safety solution designed to address these challenges. This solution includes:

- **Real-time communication:** The system ensures that the right information reaches the right people quickly during emergencies. This is achieved through mobile apps, pagers, personal alarms, digital radios, and information screens.
- **Incident management:** The solution supports both minor and major incidents, from vandalism and bullying to severe threats. It enables staff to take immediate action, minimising the impact of incidents.
- **Automated alerts:** Predefined incident scenarios can trigger automatic alerts, ensuring swift responses to emergencies like lockdowns or evacuations.
- **Public awareness:** Information screens can also be used for general announcements, helping to keep the school community informed and prepared.

By leveraging real-time communication and automated alerts, schools can better protect students and staff, creating a safer learning environment for all.



CASE: Video Surveillance

Wind farm construction in Germany

Construction sites for renewable energy projects are often located in remote areas, making them vulnerable to theft and vandalism. Traditional security measures can be costly and difficult to implement in these locations.

AddSecure's brand Video Guard addresses these challenges with a comprehensive, mobile surveillance solution powered by solar energy. Key features include:

- **Solar-powered surveillance towers:** These towers are equipped with solar panels and fuel cells, ensuring continuous, off-grid power supply.
- **Real-time monitoring:** The system provides 24/7 surveillance, with real-time video feeds accessible remotely. This allows for immediate response to any incidents.
- **Environmental sustainability:** By using renewable energy sources, Video Guard minimises the environmental impact of site security.



During the construction of a wind farm in Germany, Video Guard was deployed to secure the site. The solar-powered towers were strategically placed to cover the entire area, providing comprehensive surveillance without the need for external power sources.

The use of solar power and fuel cells reduced operational costs and eliminated the need for frequent site visits to maintain power supply. Real-time monitoring and immediate incident response significantly reduced theft and vandalism, ensuring the project stayed on schedule. The environmentally friendly solution aligned with the project's commitment to renewable energy.



CASE: Elderly Care



Improving home care in Laitila

As the number of elderly people requiring home care increased, the workload for healthcare staff became overwhelming. In Laitila, Finland, AddSecure's safety phone services have become an integral part of home care for the elderly, offering peace of mind to both the seniors and their caregivers.

AddSecure provides a safety phone system, including:

- **Emergency wristbands:** Elderly individuals wear wristbands that allow them to make emergency calls and establish voice communication with AddSecure's response center.

- **24/7 response centre:** The response centre is staffed by trained professionals who assess situations and dispatch appropriate help, such as ambulances or home care workers.
- **Door alarms:** Used in homes of elderly individuals with memory issues, these alarms notify caregivers if a door remains open during the night.

AddSecure's safety phone services have significantly improved the quality of home care in Laitila, providing a reliable and efficient solution for elderly safety. The system supports the goal of enabling seniors to live independently at home for as long as possible.



CASE: Safe Shopping Centre

Safer shopping at Frölunda torg

Frölunda Torg, a bustling shopping centre in southwestern Gothenburg, has implemented AddSecure's advanced safety solutions to ensure a secure environment for both staff and visitors. With around 200 shops, restaurants, and cafes, Frölunda Torg faces significant security challenges due to the high volume of people and activities. Ensuring safety and quick response to incidents is crucial.

AddSecure has provided Frölunda Torg with a comprehensive safety system that includes:



- **Alarm buttons:** Both fixed and portable alarm buttons are used by store personnel to silently alert the security centre in case of emergencies. This allows for immediate intervention by security personnel.
- **Structured safety work:** The shopping centre has achieved the highest safety certification, reflecting its commitment to proactive safety measures and collaboration with local authorities.
- **Rapid response:** The alarm system enables quick local interventions, preventing situations from escalating. This daily use of alarm buttons ensures continuous safety for employees.

AddSecure's tailored safety solutions have successfully enhanced the security at Frölunda Torg. The risk of incidents escalating has significantly reduced. Staff feel safer knowing they can quickly call for assistance, even in non-critical situations. Close cooperation with police and local entities has strengthened overall security efforts.



CASE: Dispatch Services



Faster response time for fire brigades

AddSecure's IT solutions for rescue services is a comprehensive support system integrated with mobile technology to enhance the operational efficiency of fire brigades. Providing a robust platform for incident management, communication, and navigation, it has enabled fire brigades to respond faster and more effectively to emergencies, realising the following benefits:

- **Enhanced response time:** By streamlining incident management and

providing real-time navigation, the system significantly reduces the time taken to respond to emergencies. This can be crucial in saving lives and minimising damage.

- **Improved coordination:** The integration with RAKEL and mobile accessibility ensures that all units involved in an operation are well-coordinated, reducing the risk of miscommunication and errors.
- **Operational efficiency:** The system's ability to manage and track incidents helps fire brigades optimise their resources and operations, leading to more efficient use of manpower and equipment.
- **Data security:** AddSecure's focus on secure communications ensures that all data transmitted through the system is encrypted and protected, maintaining the confidentiality and integrity of sensitive information.

This has not only improved the outcomes of rescue operations but also enhanced the overall safety and security of both the rescue personnel and the public.

Sustainability statement

In late 2024, the EU Commission proposed halting the Corporate Sustainability Reporting Directive (CSRD). This raised questions about the future of corporate sustainability initiatives: a setback, or a chance to refine approaches?

As we release our 2024 report, the Council has agreed to “stop the clock.” For AddSecure, this means we’re now aiming for a fully CSRD-aligned report by 2028, covering FY2027. However, our sustainability focus remains the same; making sure we’re on top of our most material impacts, risks, and opportunities.

In 2024, we enhanced our corporate management system to align with our objectives. We prioritised information security, aiming for ISO27001 certification (see page 37). We improved ESG data management, updated carbon reporting to cover the entire value chain (see page 26) and reviewed our climate transition plan (see page 28). We also introduced a new system for supply chain risk management (see page 39)

and updated our annual risk assessment, including a double materiality analysis.

In 2025, we will focus on:

- Review ESG metrics in corporate reporting and governance systems for better accountability and performance.
- Supporting product teams to incorporate sustainability into the product life cycle.
- Enhancing communication of objectives and results to meet stakeholder and employee expectations.

The CSRD has driven significant progress in corporate transparency and accountability. However, ESG is about more than reporting; it involves managing aspects that influence a company’s ability to meet its targets and taking responsibility for its impact on stakeholders. This is our ongoing commitment.



Johanna Giorgi, Chief Sustainability Officer, AddSecure

GENERAL INFORMATION P. 12

- Basis for preparation
- Our strategy
- Our business model
- Stakeholder dialogue
- Material impacts, risks and opportunities
- Governance

ENVIRONMENTAL INFORMATION P. 26

- Climate change and carbon emissions
- AddSecure’s climate transition plan
- Resource use and circular economy

SOCIAL INFORMATION P.34

- Workforce
- Customers and end-users
- Workers in the value chain

GOVERNANCE INFORMATION P.40

- Business conduct

Basis for preparation

The AddSecure sustainability statement informs and reports about AddSecure's 2024 progress and management of identified material impacts, risks and opportunities. The reporting period is January 1, 2024, to December 31, 2024. The report uses the ESRS standard as a guideline for its preparation, outline and content. The 2024 company report and sustainability statement has not been assured by any third-party assurance provider.

The materiality assessment forms the basis for the sustainability statement. The annual assessment reflects and prioritises AddSecure's most important sustainability aspects from the perspective of internal and external stakeholders. Sustainability data is collected from all business units, premises and group functions to the internal reporting system. This has resulted in a consolidated summary for the AddSecure Group. Unless otherwise stated, the data presented pertains to the 2024 calendar year.



Global commitments

By securing IoT connectivity and end-to-end solutions in a connected world, we recognise our opportunity, and responsibility, to contribute to society's sustainable transformation and the United Nations Sustainable Development Goals. Aiming to cut our direct emissions by 40% by 2030 (compared to 2021), we support the Paris Agreement. Our Code of Conduct and our Business Partner Code of Conduct are based on the core principles of the UN Global Compact and its underlying conventions and declarations within the areas of human rights, labour standards, environment, and anti-corruption.



The following general reporting principles are applied:

- The report encompasses all Addsecure's units that have employees and where ownership exceeds 50 percent.
- Data is collected as centrally as possible as to not burden business operations with additional admin, but stored back to lowest possible level (group, business unit, legal entity, solution) as to allow for better analysis and transparency.
- We expect and push partners to deliver data as part of general agreements with no additional fee, but if costs arise these are carried by the entity/function holding the contract. With regard to acquisitions, data is added as of the closing date.
- AddSecure aims for all information and data to be relevant, transparent, consistent, accurate and complete, providing an objective picture of the company's operations.
- Any specific circumstances that may have influenced the statement are reported alongside the disclosures to which they refer.

Our strategy

Our corporate strategy sets out from an understanding of the world’s need for smart IoT solutions to address the challenges of our time, while also recognising the connected society’s vulnerability in terms of connectivity and information security.

Strategic focus



Our strategy is based on interconnected objectives that we consider fundamental for our ability to deliver on our mission to make the connected world a safer and smarter place:

Achieve long-term growth

We have set an ambitious growth target of 500M€ by 2027 (from 200M€ 2023). The target reflects the potential we see in the increasing adoption of IoT, the rapid development of commercial use cases and growing cyber security concerns. Expansion is a clearly stated goal, growing existing verticals and adding new ones. Just as well, we aim for profitable and resilient growth, aiming for +30% EBITDA margin and +70% share of recurring revenue.

Profitability **33.4%**
(EBITDA): (target >30%)

Resilience **72.9%**
(Share recurring revenue): (target >70%)

Expansion **23%**
(5Y compound annual growth rate 2019-2024): (target >20%)

Build trust in our solutions

Our name is AddSecure for a reason. Only by creating trust in our solutions can we deliver on the potential IoT holds for customers and society at large. Our IoT connectivity platform, Link, plays a central role in our ambition to deliver secure IoT solutions,

integrating SIM cards into VPN clouds while also offering high level of admin control and scalability. Acquired SIMs are continuously onboarded to Link. Moreover, we invest heavily in our management system with the objective to encompass all acquisitions in the scope of our ISO certificates (9001, 14001 and 27001). Learn more about our work to build trust in our solutions on p. 37.

Employee awareness level **50%**
(% at high level): (target 75%)

SLA fulfilment **99.99%**
(Link availability): (target 99,9)

Create customer value

We serve over 70,000 customers globally. Close customer relations and understanding of their needs and experience of doing business with us are imperative to make sure we deliver value today and cater for customers’ needs tomorrow. Customer feedback (relational and transactional NPS with use NPS being underway) is measured in a unified way across the group, managed by the central marketing team with results looped back to the business units’ sales, product and management teams.

Customer relations (rNPS): **21** (target 30)

Customer service (tNPS): **46** (target 50)

Form strong and dedicated teams

Our strategy recognises our need for individuals with high levels of self-leadership and individual drive, with a joint vision and sense of purpose. We've made it a joint responsibility to actively seek to attract, develop and retain talent, defining related metrics for the monthly group KPIs and business units' reviews. To learn more about our workforce, see p. 34.

	20
Employee satisfaction (eNPS):	(target 25)
Employee development (employee development index in relation to industry benchmark):	+0.1 (target >0)
Leadership (leadership index in relation to industry benchmark):	+0.3 (target >0)
Gender equality (equality index):	0.78 (target 1)

Sustainable operations

Sustainability is at the heart of our mission, providing secure IoT solutions that enable customers to transform their operations and achieve efficiency gains. While our solutions have the greatest impact, we also focus on optimising our own operations and managing our assets responsibly.

	+11%
Carbon emissions (total scope 1-3 tCO ₂ e compared to 2023 base year):	(target -42% by 2030)
Workplace well-being (well-being index in relation to industry benchmark):	7.6 (target >0)
Supply chain management (share of key-suppliers risk assessed):	30% (target 100%)



Be yourself,
make a difference
and have fun!

Our business model – how we create value

Resources ► Business model ► Output

One company, one culture and great team-spirit

Our strategy recognises our need for individuals with high levels of self-leadership and individual drive, with a joint vision and sense of purpose. Read more about our workforce on page 34.

Assets and access to components

We run an asset-light business model and are centralising supplier management and logistics to ensure resilient supply chains. See how we aim to make more value out of less product on page 32, and how we manage supplier relations on page 29.

Strong stakeholder relations and partnerships

We rely on positive relationships with customers, suppliers, business partners, investors, industry peers and authorities. See how we engage with our stakeholders on page 17.

Financial capital

Group finance has the overall responsibility to ensure access to efficient working capital and to entertain strong relationships with financing and capital markets.



Collect data



Transfer data



Deliver action-able insights



Our secure IoT solutions provide customer value by solving complex needs, provide quick responses to events, and improve operational efficiency and productivity. By enabling data to be transmitted securely through our IoT connectivity platform for the provision of managed services, we offer differentiated end-to-end solutions tailored to meet the needs of customers in various industries.

Using cameras, wearables and other type of sensors we connect devices to the Internet. By using our IoT connectivity platform, Link, for managed SIM cards we ensure end-to-end security and administrative control through a private cloud (VPN). The Link platform is offered as a stand-alone-service but also powers our industry solutions that provide customers with actionable insights based on software services. Such services encompass an ever-growing array of applications within alarms, personal safety, transports, surveillance, smart power grids, and mobility – to just mention a few.



Customers

By offering secure IoT connectivity and end-to-end solutions, we help our customers optimise and transform their operations.

Co-workers

We offer our co-workers flexible work arrangements based on mutual values and the opportunity to make a difference in their daily work.

Investors

Benefitting from the increasing adoption of IoT, driven by trends such as big data and analytics, cyber security concerns, as well as rapid development of commercial use cases of IoT applications, we continue to innovate and grow our value.

People and planet

IoT is a key enabler to solve many of the challenges the world and organisations are facing. Our knowledge about how to securely transfer data from A to B for the provision of software-enabled services, is the very reason why AddSecure is well positioned to make a difference and contribute to society's sustainable transformation.

Our value chain

AddSecure develops and offers secure IoT connectivity and solutions. Our principal value chain is divided into three main sections:

UPSTREAM

- Supply of raw material and components,
- Manufacturing of products
- Air freight and road transports
- Financing

OWN OPERATIONS

- Product design
- Assembly of products
- Refurbishment
- Facilities and office premises
- Workforce

DOWNSTREAM

- Road transports
- Installation
- Product use
- Recycling and disposal

For an overview of identified impacts, risks and opportunities in our value chain, see page 20.



IoT connectivity platform: smarter and safer connection of devices

Our IoT connectivity platform, Link, plays a central role in our ambition to deliver secure IoT solutions, integrating SIM cards into VPN clouds while also offering high level of admin control and scalability. Our objective is to have 75% of all our managed SIM cards on Link by 2030. The IoT connectivity platform provides a complete infrastructure for management of SIM cards, data traffic, and remote access and access control, through an interface, either web or app-based, to manage and monitor the connected devices.

The user interface is intuitive and utilises a high level of automation, limiting the risk of human errors. Communi-

cations are completely isolated from other internet traffic and closed off to unauthorised users and devices. Multiple private networks can be created and managed to cater for separation of various end-customers, traffic, and systems. The IoT connectivity platform powers our different IoT solutions. IoT connectivity is also offered as a stand-alone solution to customers seeking to secure the communication of connected devices. By providing easy administration of virtual private networks, SIM cards, and access management for customers, we enable data to be securely transmitted between customer and end-user, or between customer and AddSecure for the provision of additional services.

Stakeholder dialogue and engagement

By considering impacts to external stakeholders and ecosystems in addition to those directly affecting the company we can better assess the systematic and longer-term risks that inevitably arise through these impacts.

The stakeholder dialogue is an ongoing process whereby we take into consideration stakeholders' views to identify relevant impacts, risks and opportunities (IROs). Identified IROs (topics, sub-topics and sub-sub-topics) are assessed using a double materiality approach. Depending on the subject matter and target group, stakeholders are invited to the assessment process, and/or to verify the output. For each material topic, issues have been identified that we work on in order to realise long-term results and values. A risk register is set up including information on how topics are managed and disclosed. Performance is shared to stakeholders using formal reports as well as more informal communication channels (meetings etc).

The matrix below showcases our main stakeholders, our means for engaging with these on a recurring basis, the stakeholders' expectations and requirements as well as the topics that have been identified as most relevant for each stakeholder group. We use surveys to validate our analysis with co-workers and owners. We engaged in a dialogue with internal sales and support functions to better understand our customers' expectations. Frameworks, guidelines, regulations, and other external requests for information served us to understand expectations from policy makers, rating institutions, and society in general. The stakeholder and materiality analysis is reviewed annually. For more information on risk management and materiality assessment, see p. 19.



Stakeholder overview

Who	How we engage	Requirements	Expectations	Top 3 topics of specific interest and concern
Customers and end-users	Technical and customer support, sales, surveys, web, media (incl. social media), Requests for information (RFI's)	Quality solutions and delivery on time, protected data	Simple and smooth ordering and installation process, available support when needed	• Innovation and development of products & solutions • Management of critical incidents • Management of cyber, data and information security (production)
Current and future employees	GROW meetings, yearly performance review, team meetings, town-halls, all-hands company meetings, intranet, surveys, internal trainings	Remuneration, occupational health & safety	Positive company values and culture, personal development, equal opportunities, compensation and benefits, protected data	• Employee satisfaction/health & safety • Innovation and development of products & solutions • Internal communication & information sharing
Investors, shareholders and lenders	Investor meetings, annual and monthly reports, budget and business strategy review	Transparent and adequate information sharing	Achievement of set targets	• Sales performance • Employee satisfaction/health & safety • M&A management and integration
Business partners and suppliers, bankers and raters	Joint initiatives, quality meetings, assessments, audits, reporting	Honoring contracts and agreements, legal compliance and adherence to relevant standards and guidelines, protected data	Professional and timely forecasting and ordering, clear requirements, payment on time, responsible, transparent and fair business practices	• Management of supply and value chain • Business ethics • Company reporting
Policymakers, communities and general society	Industry association memberships, media (incl. social media), external reports, CSR programs and initiatives	Legal compliance	Responsible, transparent and fair business practices	• Business ethics • Management of legal and regulatory requirements • Innovation and development of products and solutions

Material impacts, risks and opportunities

Risk management at AddSecure is about supporting our strategic objectives in the medium term and ensure our endurance in the long term. Our risk management framework is designed to enable a consistent approach to the identification, management and oversight of key risks, allowing a holistic and meaningful comparison of the risks faced and how they are managed across the company.

To identify relevant topics, we analyse macro and market trends in relation to the company's strategic direction. We consult market and industry reports as well as reporting guidelines, benchmark against industry players and sustainability forerunners, and engage with our stakeholders. To assess impacts, risks, and opportunities on group level we use focus groups consisting of internal stakeholders and experts throughout the organisation, gathered around five central themes: governance, information security, environment, workforce, and business development and performance. These internal focus groups are tasked to define relevant sub-topics within each theme and assess these with regards to financial and impact materiality, performance, and mitigation measures in place.

The assessed topics are documented in a risk register, mapped to AddSecure's main processes and assigned to an owner responsible for monitoring and mitigation of the topic/risk. The IRO assessment is up for review in the Corporate Management Team, discussing identified impacts, risks and opportunities, KPI performance, mitigation measures and proposed actions. The management review is presented annually to the Audit Committee and the Board of Directors.

The management review forms the basis for the Corporate Management Team's annual strategy deep dive where main prioritisations for the coming year are made. The management team's strategy review is followed by budget discussions held with group functions and business units' management teams. Once the budget is approved by the Board, the commitment setting process starts on team and individual level. This way we ensure that the strategy stays relevant and takes into consideration the whole company's knowledge base. By letting the strategy review form the basis for the budget and commitment setting procedures, we make certain that there's a clear line between what we want to achieve (strategy), the dedication of resources (budget) and execution (commitments).

Operating within the area of IoT connectivity and end-to-end solutions, cyber, data, and information security is identified as a highly material topic along the value chain, from an impact as well as a financial point of view. Data intrusion, downtime or loss of data, failed GDPR compliance, theft of digital assets, and lack of security in product design are all aspects linked to AddSecure's ability to create trust in our solutions (see page 37). Accordingly, the operational ability to manage incidents and service outages is assessed as highly material, not least from a customer point of view.



UPSTREAM	OWN OPERATIONS	DOWNSTREAM
IMPACTS	Growing portfolio of secure IoT solutions - Optimised use of energy & resources - Reduced CO₂ emissions - Reduction of asset depreciation and waste - Enhanced public & individual safety - Reinforced digital infrastructure CO₂e emissions from AddSecure's operations	
RISKS	Cyber attacks & information security breaches 3rd party vulnerabilities - Down-time in operations - Data-intrusion, loss of data, corrupt data - Down-time in critical infrastructures - Data-intrusion, loss of data, data corruption - Supply chain disruptions and increased COGS due to more frequent extreme weather events and increased competition for materials and components - Reputational, legal, purchasing & financial risks related to adverse impacts in the supply chain - Extreme weather events damaging physical assets - Increased costs for legal compliance - Lack of competence and loss of key-personnel - Non-sufficient R&D capabilities and resources - Access to financing	
OPPORTUNITIES	Improve access to talent through strong value proposition and employer brand	- High info sec standards leading to competitive advantage - Increased demand for IoT solutions to improve, manage & report ESG performance - Increased demand for secure connectivity solutions

The understanding of risks within the supply and value chain (see page 39) has broadened from previous years, highlighting not only access to components and human rights issues, but also identifying third party information security vulnerabilities as a material risk. The trend is that supplier due diligence is primarily driven from an operational and risk management perspective, going beyond legal compliance.

As a service-oriented company, our climate impact is relatively limited. As we extended our carbon reporting and updated our climate transition plan, it became however increasingly clear how the carbon emissions are closely related to the realisation of strategic objectives and optimisation of operations. Learn more in the section on Climate change (page 26).

All in all, topics identified as material and included in the annual assessment correspond well to AddSecure's strategic focus areas (see page 13). More information about relevant policies, actions, targets and metrics are to be found in the sections Customers and end-users (page 37), and Workers in the value chain (page 39). See also specific sections on Climate change (page 26), and Workforce (page 34). Current measures in place to manage risks and opportunities are for all topics deemed efficient or moderately efficient. Need for improvements have been identified related to legal compliance, critical incidents, GHG emissions, use of resources, cyber and information security, and innovation are deemed to be moderately effective. See each of these topics for more information.

Material aspects

Overview of material topics, sub-topics and related management processes identified in the 2023 double materiality assessment. AddSecure continues to develop its DMA process to align with the ESRS standard.

	Topic	Sub-topic	Related processes	Description
GOVERNANCE	Internal communication and awareness		Lead & control the business, Organise & develop employees	Need for efficient communication to create engagement, support decision making and achieve objectives.
	Legal compliance		Lead & control the business	Increasingly complex regulatory environment and specific customer requirements increases the need for resources for legal compliance and product documentation.
	Supply & value chain	Due diligence of suppliers	Manage suppliers & contracts	Reputational, legal, purchasing & financial risks related to adverse impacts in the supply chain
		Cost optimisation & sourcing	Manage suppliers & contracts	Increased competition and geo-political uncertainties impacting access to components.
	Business ethics	Anti-corruption, fair business practices	Lead & control the business, Manage suppliers & contracts, Organise & develop employees	Risk for unethical behaviour in business relations, foremost in sales and procurement.
		Respect for human rights and labor rights	Manage suppliers & contracts	Primarily related to supplier management and due diligence of suppliers (see separate entry).
ENVIRONMENT	Business continuity	Managing critical incidents, incl service outages	Operations of products & services	Lack of understanding on how to handle and manage critical incidents or crises can worsen the situation instead of effectively mitigating it.
	Climate change	GHG emissions	Lead & control the business, Operations of products & services, Product life cycle management	Increasing regulations and stakeholder expectations on companies to manage and report GHG emissions and climate mitigation.
		Climate change impacting company performance and value chain	Lead & control the business, Manage suppliers & contracts, Operations of products & services, Product life cycle management	A changing climate and more frequent severe weather events increase the risk for physical assets, including production platforms, and interrupted logistics/supply chains. Warmer temperatures may lead to safety and health risks impacting the workforce. The need for energy and resource efficient solutions likely to increase, as well as the need for solutions helping customers to manage their climate impact.
	Use of resources	Access to components	Manage suppliers & contracts, Product life cycle management	Increased competition and geo-political uncertainties impacting access to components with risk for increased COGS and reduced margins. Purchased goods closely related to GHG performance.

	Topic	Sub-topic	Related processes	Description
INFORMATION SECURITY	Cyber attacks and information security breaches	Data-intrusion and loss of data	Business system management, Operations of products & services	Security breaches and operational downtime constitute a significant risk for our critical infrastructure.
		Information related impacts on consumers and end-users	Operations of products & services, Product life cycle management	Security breaches and operational downtime constitute a significant risk for customers' critical infrastructures.
		3rd party vulnerabilities	Operations of products & services, Product life cycle management, Manage suppliers & contracts	Accidental or built-in vulnerabilities in purchased goods and components.
	Data privacy	Personal data (PII)	Product life cycle management, Operations of products & services, Organise & develop employees	Personal Data (PII) being shared, either on purpose or by accident, without consent or legal justification.
		Classified information	Product life cycle management, Operations of products & services, Organise & develop employees	Data being shared, either on purpose or by accident, with unauthorised parties.
	Data quality		Product life cycle management, Lead & control the business	Human behavior, technical settings or software design causing data corruption (accidental or deliberate).
WORKFORCE	Attract talent		Organise & develop employees	Using diversity as a mean to widen the talent pool and improve innovative capabilities.
	Employee development and training		Organise & develop employees	Insufficient investment in employee development and training could decrease employee performance and productivity, increase turnover rates, reduce employee engagement, increase risk of errors, and slow down innovation and change.
	Employee satisfaction & engagement		Organise & develop employees	Non-satisfied employees could have a negative impact on company performance and brand.
MARKET & INNOVATION	Financial management	Economic downturn, inflation and currency risks	Finance management	Risk of cost increases and price erosion driven by inflation that could impact customer investments and activity.
		Interest levels and hedging	Finance management	Vulnerabilities due to debt levels.
		Taxation	Finance management	
		Company reporting	Finance management, Lead & control the business	Financial and non-financial (eg CSRD and EU taxonomy) reporting guidelines keep evolving
		M&A management	Manage mergers & acquisitions	Failing to successfully integrate acquired assets could lead to missed synergies, operational risks and value depreciation.
	Innovation & development	Legacy & migration	Product life cycle management, Operations of products & services, Sell products & services	Closing down legacy platforms can free up R&D resources but brings a risk for customer churn in connection to platform migration.
		R&D investments and Capex spend	Product life cycle management	Unsufficient R&D investments negatively impacting competitive edge and customer satisfaction.
		Customer insight, value and impact	Lead & control the business, Product life cycle management, Sell products & services	Lack of insight into customer needs and demands deteriorating competitive edge and customer satisfaction.
		IP rights	Marketing, Product life cycle management	Risk for trademarks being violated, or AddSecure violating trademarks.

Governance

Efficient management is crucial for reaching our long-term objectives. To stay close to customers and local markets, we run a partly decentralised organisation. While the Board of Directors, the CEO, and the Corporate Management Team hold central functions, Business Unit Presidents are responsible for attaining objectives set within each business unit and manage customer facing processes, operations and R&D. Chief Officers are responsible for managing cross-vertical organisational support and development, set up and manage joint structures (processes, KPIs, business systems, joint services) throughout the group with the aim to achieve synergies and optimise operations.

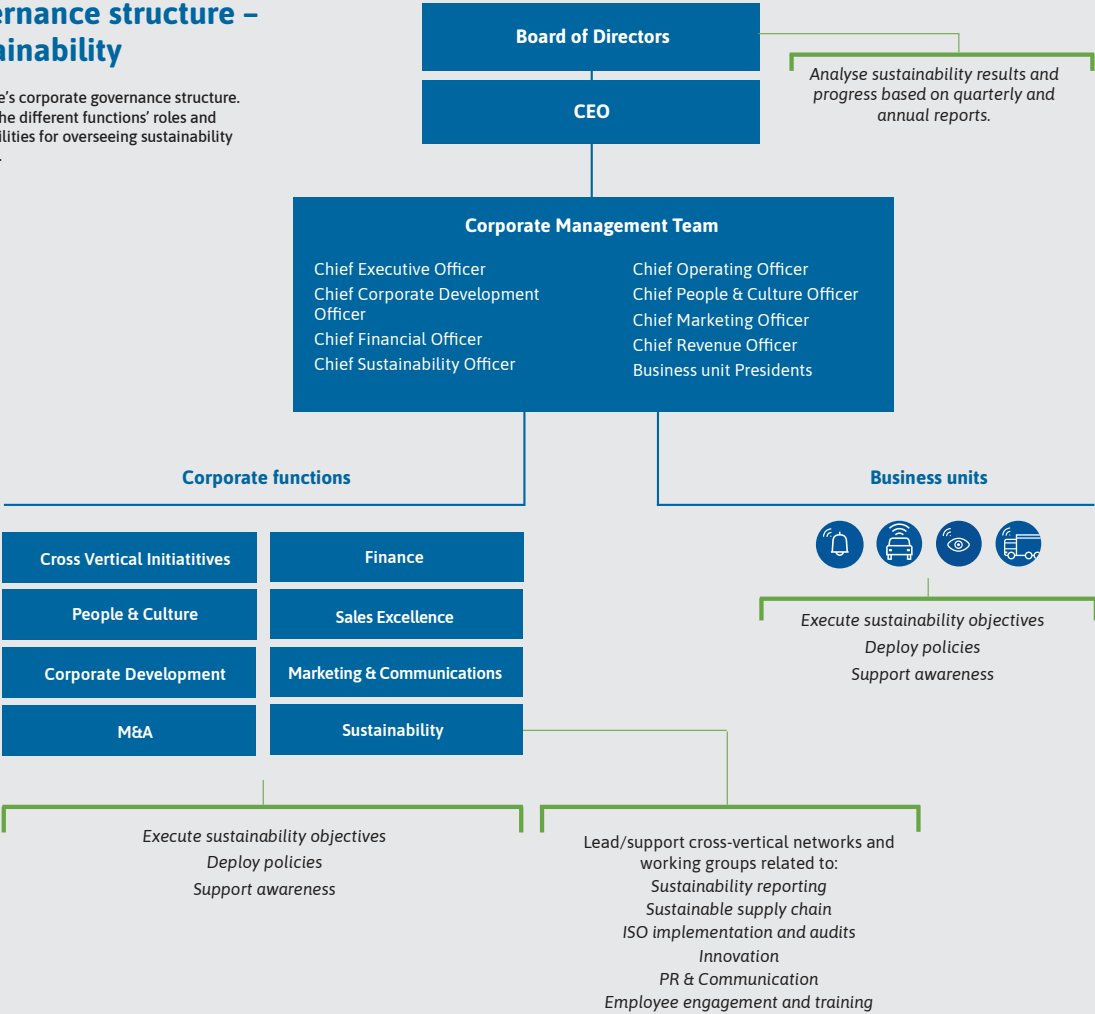
AddSecure’s sustainability program is organised as a central function, mandated to lead the development and implementation of a company-wide sustainability strategy. The objective is to integrate sustainability across business units and throughout the company as an accelerator of strategic growth and long-term value creation. The work is led by the Chief Sustainability Officer who is part of the Corporate Management Team and reports directly to the CEO.

Sustainability related incentive schemes

Non-financial metrics, such as CO₂ emissions, energy use, circular performance and employee satisfaction and commitment, are included in monthly reports to the Board. In 2024, performance indicators for long-term business value were defined. Incentive scheme principles for senior executives, including the CEO and other members of Corporate Management Team, are to be reviewed as to investigate the possibility to link variable remuneration to the long-term business value performance. Decisions on the design of the incentive programs and the adoption of outcomes are taken by the Board.

Governance structure – Sustainability

AddSecure’s corporate governance structure. In italics the different functions’ roles and responsibilities for overseeing sustainability processes.





Guidelines and policies

Through the Group Policy Portfolio, AddSecure’s core values and way of working are established. All Group Policies are approved by the Board of Directors.

- Code of Conduct
- Business Partner Code of Conduct
- Corporate Governance Policy, including Governing Documents Guideline and Risk Management Guideline
- Sustainability Policy
- Finance Policy
- IT Policy
- Information Security Policy
- Data Protection Policy
- People & Culture Policy
- Communication Policy
- Purchasing Policy

Sustainability framework

As a “meta” megatrend sustainability has an influence on all industries through the current or future megatrends that can be observed or predicted. As such, sustainability impacts customer demands as well as our own operations.

Our sustainability program covers the whole AddSecure Group and rests on three main pillars: governance, transparency, and business development. It is designed to manage and integrate sustainability throughout the organisation, while also creating a structure to help us improve our ability to efficiently respond to changing stakeholder demands.

Our sustainability program forms an integral part of the corporate strategy. Striving towards the vision to make the connected world a safer and smarter place by providing secure IoT solutions that help transform and optimise customer operations put sustainability at the very core of our mission.



Climate change and carbon emissions

Governance

The changing climate causes more frequent natural disasters and severe weather events, leading to risks for physical assets, interrupted logistics/supply chain, and increased cost. Warmer temperatures may also lead to safety risks and diseases impacting workforce health and/or ability to work. On the other hand, heightened risk of extreme weather is expected to increase the need for strong, resilient communications networks.

To further our understanding of long-term climate related risks and opportunities within the context of a changing climate, we're reporting in accordance with the EFRAG guidelines to meet the requirements of the Corporate Sustainability Reporting Directive (CSRD). As part of our sustainability framework, climate mitigation and adaptation are governed by the Group's Code of Conduct and Sustainability Policy. Climate related metrics, on group and business unit level, are included in the quarterly and annual reports presented to the Board and the Corporate Management Team. Climate related impacts, risks and opportunities are reviewed in the group's annual materiality and risk assessment, informing decisions on actions to meet our climate related targets.

To accurately assess our impact and set clear milestones for emissions reduction, we updated our GHG assessment methodology in 2024. This now includes emissions from



As the world becomes increasingly digitalised, information and communications technologies, data centers and network services are emerging as an important source of energy demand. The current environmental footprint of the ICT sector is estimated to be between 5% to 9% of the world's total electricity use and more than 2% of all emissions.

purchased goods and services, one of our key emission hotspots, along with improved data coverage and refined accounting principles. The 2023 baseline data presented in the 2024 report have been updated in line with updated accounting principles, this to allow for comparison over time.

Strategy

Technology plays a significant role in addressing climate change, with the World Economic Forum estimating that digital solutions, if brought to scale, could reduce global emissions by 20% by 2050.¹

AddSecure's IoT solutions enable customers to optimise energy use, reduce waste, and lower emissions by providing intelligent (smart), connected technology that enhances efficiency and sustainability. At the same time, we acknowledge that producing, installing, and maintaining our products and solutions come with an environmental footprint that we are actively working to minimise.

Climate related impacts, risks and opportunities

Climate-related risks and opportunities have been analysed using SSP1-1.9 for transition risks and opportunities, which meets the Paris Agreement's 1,5°C target. For assessing physical risks, SSP5-8.5 was utilised, which anticipates a 4.4°C or higher increase in average global temperature by 2100. The scenario source used was UN Intergovernmental Panel on Climate Change (IPCC) 2021. Additionally, short-term, medium-term and long-term time horizons were followed when analysing the climate-related risks and opportunities.

Physical climate risks have a potential negative impact on AddSecure's operations, such as extreme weather causing interruptions in supply chains, operations, premises and service delivery. However, mitigation measures in place are deemed effective. Material risks and opportunities are rather found within the transition to a low-carbon economy. We already see increasing demands from customers, business partners and financial actors for more detailed information and quality data related to carbon management and strategies. Demands that request dedicated resources to fulfil. However, as our customers are facing similar demands and legal obligations, we see an increasing surge for sustainable digital solutions that can support customers in their quest to optimise operations and lower emissions through automated processes and quality insights.

The findings from the analysis are integrated in AddSecure's annual risk management system and evaluated annually. For more information, see page 19.

¹ <https://initiatives.weforum.org/digital-transformation/digital-and-climate>

AddSecure’s climate transition plan

Our Climate Transition Plan reflects our ambition to align with global climate goals. It focuses on our own operations across the value chain, presenting the following objectives:

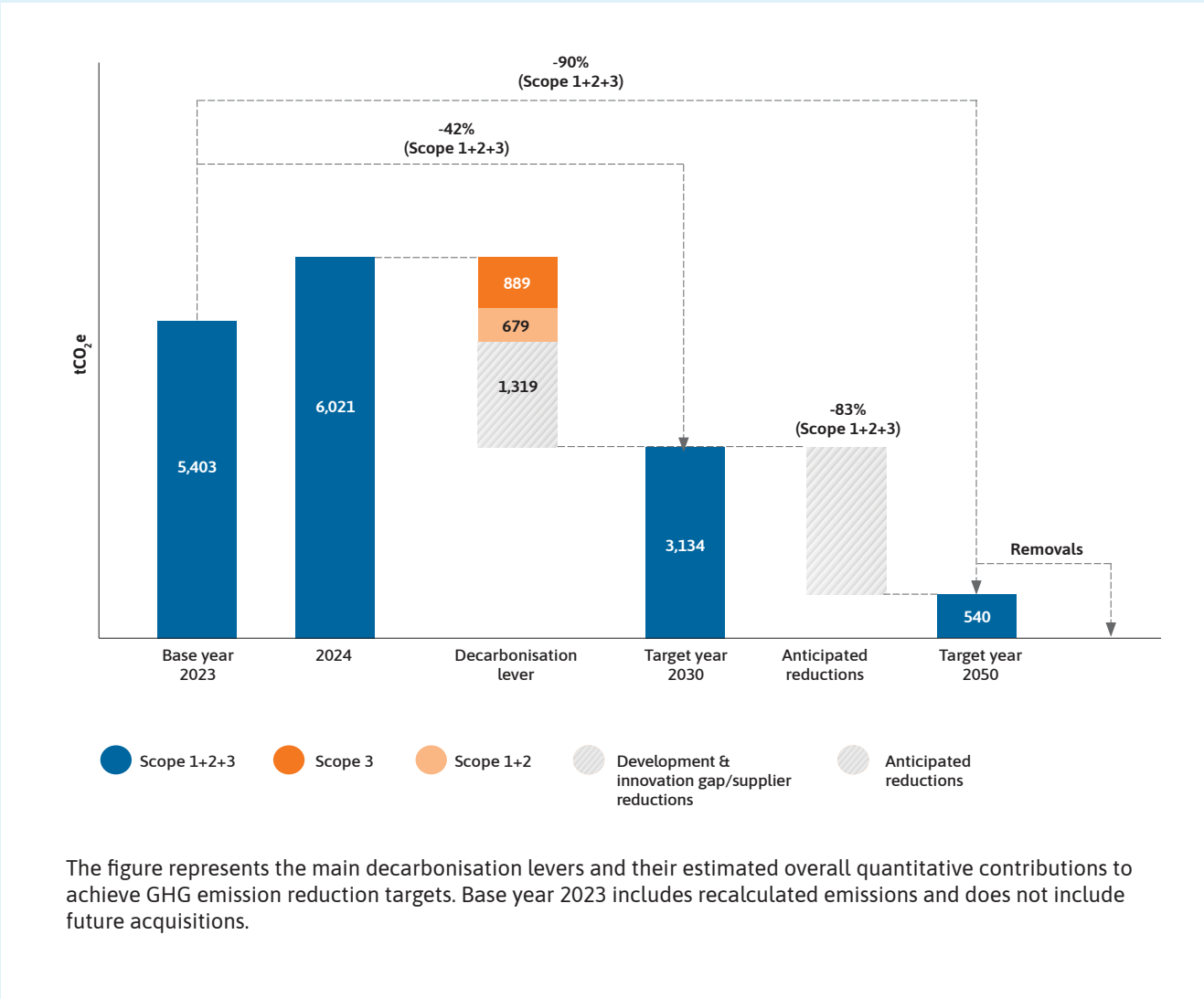
- Achieve net-zero GHG emissions across our value chain by 2050.
- Reduce GHG emissions from our value chain by 42% by 2030, using 2023 as the baseline.
- Reduce Scope 3 emissions per unit value (revenue) by 51,6% by 2030 from a 2023 base year.

Our transition plan aligns with the Paris Agreement’s 1.5°C target and is built upon previous work around the TCFD recommendations. The 2030 emission reduction goals have been developed using the Science-Based Targets initiative (SBTi) methodology.

Actions and targets

Scope 1

Company vehicles is our main source (94%) for direct emissions. To **decarbonise our vehicle fleet**, we are significantly increasing the adoption of hybrid and electric vehicles within our company car portfolio. Our target is for 95% of our company cars to be electric, hybrid, or plug-in hybrid, compared to 21% in 2023. This transition will contribute to a 26% reduction in emissions from this category, aligning with



our broader commitment to reducing transportation-related emissions.

Scope 2

To lower the climate impact from purchased energy we are enhancing the sustainability of our office premises by improving energy efficiency and transitioning to renewable energy sources. We aim to optimise office space utilisation by reducing the area per employee from 13.7 m² to 8 m², while simultaneously ensuring that 100% of our office and warehouse electricity comes from renewable sources, an increase from 83% in 2023. These measures will contribute to lowering our operational footprint while promoting resource efficiency.

Scope 3

Optimising transportation and distribution is a key focus area, particularly in air freight. We want to ensure that 80% of our air freight uses sustainable aviation fuels, which will play a critical role in reducing emissions from logistics and supply chain operations.

A digital-first policy is at the centre of our **business travel** reduction strategy. By leveraging virtual collaboration tools and implementing stricter travel policies, we are targeting a 55% reduction in the total kilometres travelled for business purposes. This shift is expected to result in a 68% decrease in emissions from business travel.

For more information about our strategy to create more value out of less products, see page 32.

Employee commuting is another important source of emissions and where we are taking action for change. Compared to 14% in 2023, we are now aiming for 85% of all employee commutes to be made using public transport or electric and hybrid/plug-in hybrid cars. In parallel, we have an active hybrid workplace allowing employees to work from home which further reduces the need for daily commuting. Together, these initiatives are expected to cut emissions from employee commuting by nearly half, demonstrating our commitment to making low carbon commuting the standard within our organisation.

Finally, but certainly not least, reducing emissions from **purchased goods and services** is a key priority. 48% of our total emissions stem from purchased goods and services. Our target is to reach a 65% reduction by 2030.

Understanding the strategic long-term business value of an asset light business model, AddSecure has set the strategy to Create more value out of less product. Promoting recurring revenue streams, software-based offerings, efficient inventory planning, eco-design of products, forming of strategic OEM partnerships and reuse of products and components, the strategy is designed to help us develop new revenue streams, decouple growth from hardware use, address risks in the supply chain, reduce costs of goods sold, and reduce adverse environmental impact.



2024 performance

About the data

The 2023 tCO₂ emissions have been accounted for using the GHG Protocol principles. Activity data related to scope 1 and 2 emissions include all relevant GHG categories. Scope 3 emissions include GHG emission categories purchased goods and services (data storage), transport and logistics (upstream/downstream), leased assets, business travel and employee commuting.

In 2024 we conducted a full review of our emission data, adding purchased goods to the reporting. We recalculated our base year (2023) emissions, using updated methodologies. 96% of the 2024 emissions have been calculated using activity data, 4% were calculated using a spend based analysis.

Progress and insights

In short, we are off track to meet our 2030 short-term targets. Even if our GHG intensity (emissions per revenue) decreased, in comparison to 2023, total 2024 emissions increased with 11%, taking us further away from the main target to lower our emissions by 42% by 2030. Purchased goods and services is our main emission source. The rapid growth of our operations, and the migration to 5G calling for an exchange of many of our customers’ devices, has increased the demand for purchased components and related logistics. Emissions associated to cloud data storage is growing in importance as data is moved from own data centres, which however is mirrored in decreased emissions within scope 2. Business travel increased in 2024 (foremost long-haul flights), as well as emissions related to employee commuting (increased use of cars for commuting).

Metrics and targets

	2024	2023	Target
Total emissions (tCO ₂ e)	6,021	5,403	3,134 (-42%)
GHG intensity (tCO ₂ e/M€)	26.3	27.0	13.06 (-51,6%)
Emissions per capita (tCO ₂ e/FTE)	6.23	6.05	-
GHG removals	0	0	-
Tonnes offset (tCO ₂ e)	0	0	-
Energy consumption in own premises (kWh)	1,634,663	4,798,344	-
Share renewable electricity of total purchased electricity	85%	82.8%	100%

Scope 1 and 2 emissions differ greatly between 2023 and 2024, mainly due to updated accounting principles and the introduction of new data sources impacting emissions related to combustion and purchased energy. Car related emissions kept decreasing in 2024 (-6% compared to 2023) as the share of hybrid, plug-in and electric vehicles kept growing. At year end, hybrid, plug-in and electric vehicles constituted 42% of total kilometres travelled, to be compared to 26% in 2023.

We predict that the 4G migration will flatten out by 2027, leading to a decrease of emissions related to the exchange of devices. However, to further reduce emissions related to purchased goods and services – identified as a key priority in our climate transition plan – we need to explore and

strengthen data-driven and recurring revenue streams. The group’s strategy to create more value out of less product is therefor just as much key to ensure long-term growth as it is to lower the group’s emissions (for more information about how we look to create more value out of less product, see page 32).

During 2025, selected carbon metrics (related to vehicles, business travel and purchased goods) will be included in the business units’ business reviews. This to create ownership for both long-term and short-term actions defined in the climate transition plan. Other areas, such as energy use in company premises, employee commuting and the development of new revenue streams, will be supported centrally as cross-organisational initiatives.

2024 emissions

Category	Base year 2023 (tCO ₂ e)	2024 (tCO ₂ e)	Change, %
Scope 1 GHG emissions			
Stationary combustion & fugitive emissions	9	63	>100
Company cars	1023	964	-6
Gross Scope 1 GHG emissions	1032	1027	-0.5
Scope 2 GHG Emissions			
Purchased electricity	191	231	21
Heating & cooling	362	64	-82
Gross Scope 2 (location-based) GHG emissions	553	295	-47
Gross Scope 2 (market-based) GHG emissions	496	210	-58
Scope 3 GHG emissions			
Purchased goods & services	1589	2494	57
Capital goods	674	436	-35
Fuel & energy related activities (not included in Scope 1 or Scope 2)	147	128	-13
Transportation & distribution (upstream & downstream)	180	253	40
Waste generated in operations	85	112	32
Business travel	484	518	7
Employee commuting	639	749	17
Downstream leased assets	12	9	-25
Gross Scope 3 GHG emissions	3818	4699	23
Total GHG emissions (location-based)	5403	6021	11
Total GHG emissions (market-based)	5346	5936	11

Resource use and circular economy

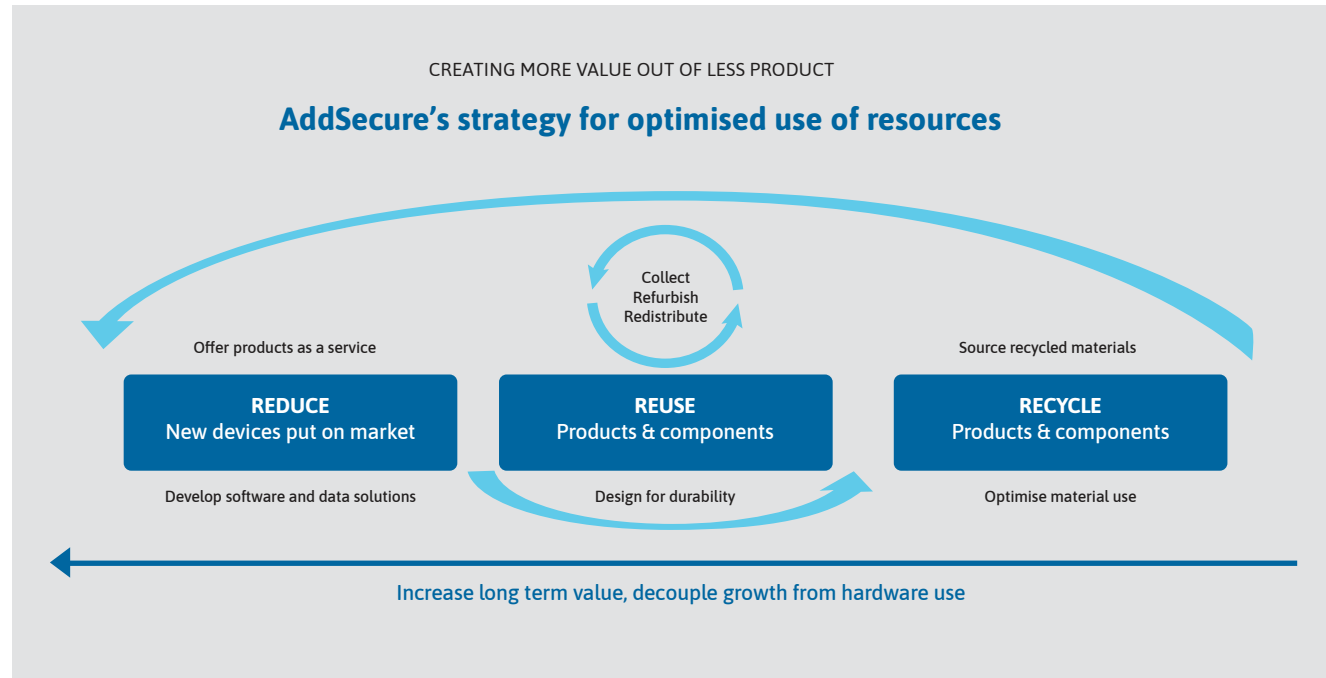
Governance

We operate a subscription-based business model with a high share of recurring revenue (>70%) for predictable and stable revenue over time. Our business model is asset-light and instrumental to our ability to grow long-term customer relations and secure profitability and growth, even during economic and geo-political turmoil and growing resource constraints. “Creating more value out of less product” is set as a strategic focus and part of the overall business strategy and the M&A process. By working for a smarter use of resources we expect to lower our environmental impact while also cutting costs of produced goods and improve risk management in our supply chain.

During 2024 we’ve continued to develop our strategy on group level, reviewing joint KPIs in monthly management reports that connect to the business rationale while also reflecting the environmental performance.

Strategy

Waste of electrical and electronic devices is one of the world’s fastest growing waste streams, while production of modern electronics requires the use of often scarce and expensive resources. In the last few years, we’ve seen the shortage of components grow in importance, posing an increasing risk to business operations. For AddSecure, purchased goods and components also represent the most significant source for climate related emissions.



Service-based profit models are recognised as key for society’s transition into a circular and climate efficient economy. Service-based models are attractive for businesses to handle growing resource constraints and shifting consumer attitudes towards ownership and consumption. Examples of circular principles such as virtualisation, sharing, and looping are already to be found within our offerings, allowing for recurring revenue that’s disconnected from the hardware life-cycle and that’s subject to low customer churn.

Looking ahead, AddSecure aim to put even greater emphasis

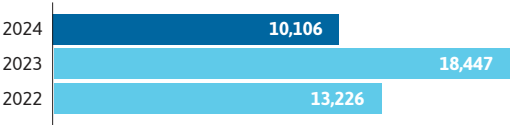
on the virtualisation of products and software-based revenue streams, decoupling revenue growth from hardware use. The M&A process will play an important role as we aim to increase our non-material (i.e. software based) revenue share. Moreover, we look to enter strategic partnerships with selected OEM partners to integrate our software solutions in partner devices. This will allow for us to further virtualise our offer, address supply chain related issues, lower our COGS all while also lowering our environmental impact related to raw materials, manufacturing, transport and distribution, and waste.



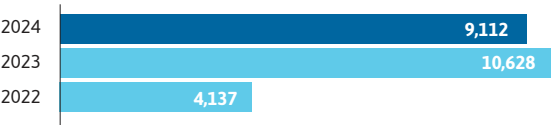
Metrics and targets

	2024	2023	2022
Recurring revenue (% of total revenues)	72.9	76.8	77.3
Non-material value creation (%)*	6.0	5.1	5.7
Products put on market	74,985	177,982	101,497
Products redistributed	10,106	18,447	13,226
Products recycled	9,112	10,628	4,137

Products redistributed



Products recycled



*Total revenue/(non-recurring COGS + CAPEX customer equipment)

Metrics and targets

As a consequence of the ongoing technology shift and customers migrating from 2G/3G to 4G/5G networks, sales of hardware (e.g. alarm transmitters) increased while the share of recurring revenue decreased. In parallel, non-material value creation (revenue as a share of the cost for purchased non-recurring customer equipment) improved. The 2G/3G sunsetting is expected to have a continued impact on our business until at least 2027.

During 2024 a new ERP system for central warehousing was put into place to help improve data quality and insights to product streams, from manufacturing to customer delivery, take-back and redistribution. Moving forward we continue to work on increasing internal awareness and understanding of circular business performance and how this is supporting bottom line results. We continue to set up and improve processes to ensure that producer responsibility is met within different geographies and legal entities. During 2025 we are introducing updated metrics for management reports and business reviews.

Sunsetting of 2G and 3G networks

The telecommunications landscape is undergoing a significant transformation with the sunsetting of 2G and 3G networks across Europe. The adoption of 4G and 5G technologies will unlock new opportunities for innovation and efficiency, particularly in the realm of IoT.

The shutdown of 2G and 3G networks has significant implications for various sectors, particularly those relying on legacy communication systems. Security and alarm systems, fire detection, and monitoring solutions are among the critical systems affected. These systems must be upgraded to ensure continuous operation and prevent potential failures.

As organisations upgrade their systems, they can look forward to enhanced capabilities and improved performance in their communication networks. AddSecure is at the forefront of this transition, ensuring that critical communications systems remain operational during and after the switch.

Workforce

Governance

People & Culture is a group function, tasked to ensure adequate workforce related processes and to build a strong company culture. P&C is responsible for the overall work environment, including monitoring, and wellness measures. Respective managers are responsible for reviewing employees' work situations. All AddSecure employees are covered by the systematic work environment agenda, managed by P&C.

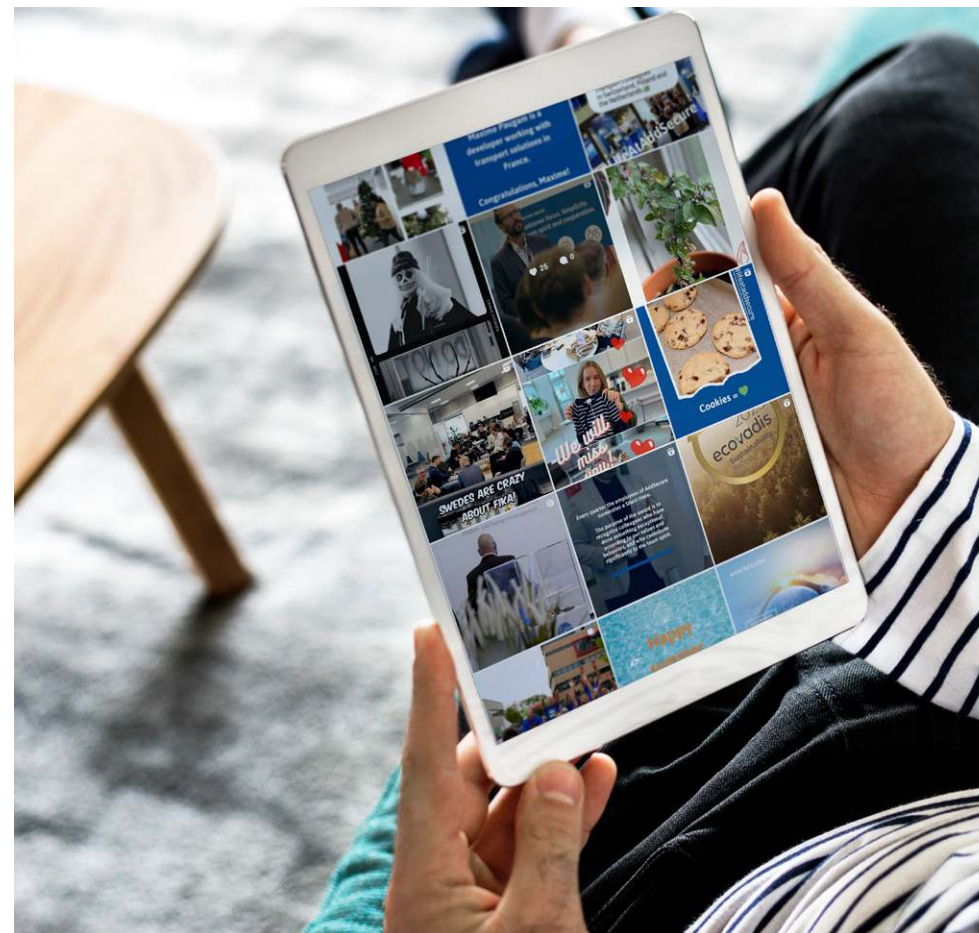
We use pulse surveys to monitor issues related to our workplace and culture, including commitment, equal opportunities, freedom of harassment and satisfaction. We train all our leaders in using the tool to develop their teams, their own leadership and to address issues of concern early on. This way, employees are given the opportunity to share thoughts and comments on a recurring basis. For those who want to ensure absolute anonymity we have established a third party operated whistleblower system, creating a safe environment where employees (and stakeholders outside AddSecure) can share information about issues they believe are not in line with company policy and culture.

Having geographically, structurally, and culturally diverse teams with different areas

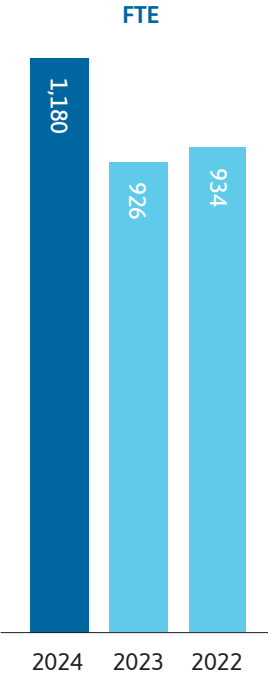
of responsibilities, our leaders are crucial to relay common values and goals. To support our leaders as “ambassadors” we operate a mandatory leaders program including aspects such as managing diverse and remote teams, dilemmas, culture etc. Culture forms an integral part of the annual, global pay review where “behaviour” and “living our values” are integrated in the performance assessment. Employee engagement and commitment (eNPS) is a central target and part of the KPIs used for BoD reporting and business reviews.

Strategy

Form strong and dedicated teams is set as one of our strategic focus areas (see page 14). Our employee proposition underlines IoT's potential to contribute to society's sustainable transformation, inviting our co-workers to a workplace where they can "be themselves, make a difference and have fun". Seeing diversity as key for innovation we actively look to increase the level of diversity in our workforce on all levels in terms of gender, age, and background, following up through several key indicators. With growth being a defining feature of the AddSecure journey, our culture plays a significant role in welcoming colleagues to the group. Building "one company, one culture" is a significant part of the company strategy.

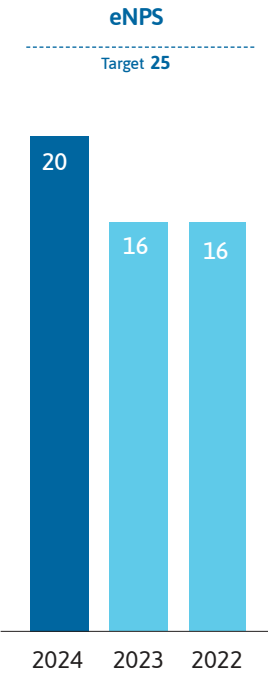


Metrics and targets



	2024	2023	2022	Target
Workforce characteristics				
Total number of employees	1,108	926	934	
Full time equivalents (FTEs)	965	819	849	
Gender distribution (% women/men/non-binary)				
Board	14/86	14/86	14/86	40/60 ratio
CMT	25/75	25/75	25/75	40/60 ratio
Leaders	23/77/0	28/71/1	26/74	40/60 ratio
Employees	31/69/<1	31/68/1	32/68	40/60 ratio
Gender equality (number of female/male managers in relation to number of female/male employees)	0.7	0.9	0.8	1.0
Average age (women/men)	40/43	39/44	39/42	-
Number of permanent employees (women/men/non-binary)	283/702/5	231/529/5	232/600	
Number of temporary employees (by gender)	22/33/1	21/23/3	22/18	
FTEs (women/men/non-binary)	213/666/2	201/567/4	218/595	
Non-guaranteed hours (women/men/non-binary)	42/18/2	35/18	43/19	
Part-time employees (women/men/non-binary)	134/87/6	59/34	79/42	

Metrics and targets



	2024	2023	2022	Target
Training and development				
Employee development	7.3 (+0,1)			>industry benchmark
Average number of training hours per employee	98			
Employee well-being and satisfaction				
Personnel turnover	17.4	17.2	19.5	
No. of employees per manager	6.8	6.8	7.0	-
Leadership	8.1 (+/-0)	8.0 (-0.1)	8.1 (+/-0)	>industry benchmark
Employee satisfaction (eNPS)	20	16	16	25 (2025)
Workplace well-being	7.6 (+0.3)	7.3 (-0.1)	7.5 (+0.5)	>industry benchmark
Personal development	7.1 (-0.1)	7.0 (-0.2)	7.3 (+/-0)	
Part-time employees (women/men/non-binary)	134/87/6	59/34	79/42	
Health and Safety				
Percentage of employees covered by health and safety management system (based on head count)	100	100	100	
Number of work-related accidents	0	0	0	
Number of fatalities as a result of work-related injuries/ill health	0	0	0	

Customers and end-users

Customer value

We serve over 70,000 customers globally. Our solutions address customers' challenges within often complex and regulated areas which require significant know-how and experience, often in a national context. Our customers often rely on our solutions to safeguard critical infrastructures. Close customer relations and understanding of local markets is therefore of utter importance. Moreover, as our solutions are based on connected devices, it is of utter importance to make sure that data and information are handled in a secure way. Delivering customer value is set as strategic objective with relevant metrics related to customer satisfaction is followed up on across the group (see page 13).

Information security

Cyber threats seeking to damage data, steal digital assets, or disrupt digital life in general, are constantly evolving. Operating in the space of the connected world, creating trust in our solutions is fundamental. Only by creating trust in our solutions can we deliver on the potential IoT holds for customers and society at large.

Governance

In 2024 we achieved an ISO/IEC 27001:2022 certification for the entire Smart Alarms business unit's operations across Europe and all corporate functions within the group. This was the first step towards a group-wide certification against the new cyber security and privacy protection version of the ISO 27001 standard. During 2024 we continued to work towards extending the certificate to the rest of the group.

The ISO 27001 framework provides a systematic approach to managing sensitive company information, ensuring its

confidentiality, integrity, and availability within AddSecure's Management System. ISO 27001 ensures that adequate security controls are in place to protect information from corruption or loss and establishes robust procedures to prevent data security breaches and theft, as well as identifying, controlling, and managing risks to the security of information assets. Data privacy and protection of personal data is an integrated aspect in AddSecure's security framework. The operational work is tied to our Information Security Forum and our management system, covering policies, guidelines, processes, metrics and targets. The Information Security Forum is an internal network established to provide strategic and practical guidance, foster collaboration, and promote a proactive approach to information security management.

Strategy

In response to the growing threat landscape, we seek to install a proactive approach to cyber security. Offensive testing, encompassing real-time defence mechanisms and robust tech barriers (including our own IoT connectivity platform, see page 16) are applied to fortify our defences against cyber threats.

We recognise the role of human error in perpetuating cyber breaches. A significant portion of corporate data breaches stems from employee mistakes or malicious intent. Phishing scams, malware downloads, weak passwords, and negligence toward security protocols contribute to breaches, highlighting the urgent need for enhanced cyber security awareness among our workforce. To this end we have implemented a digital training program consisting of micro trainings and attack simulations. The training program targets all employees and is followed up in a regular basis.

Assessing digital solutions' net climate impact

There's a need for a common framework for assessing the environmental benefits and net impacts of digitally enabled solutions. This to make for greater transparency and build credibility within the industry and among users. The European Green Digital Coalition (EGDC) is an initiative aiming to maximise the sustainability benefits of digitalisation. The EGDC pilot project provides science-based methods to estimate the net environmental impact of real-life digital solutions across sectors six priority sectors (Energy/Power, Transport, Smart cities, Construction/Buildings, Manufacturing and Agriculture). AddSecure's transport management solution Logic TMS was selected by the EGDC as a case study in 2023. Based on the developed methods, the EGDC pilot project will create recommendations for green digital transformation across sectors and promote a widespread take-up by industry players.

To read more about the EGDC and the proposed methodologies, see www.greendigitalcoalition.eu.

Our IoT connectivity platform, Link, plays a central role in our ambition to deliver secure IoT solutions, integrating SIM cards into VPN clouds while also offering a high level of admin control and scalability. Our objective is to have 75% of all managed SIM cards on Link by 2030. Acquired SIMs are continuously onboarded to Link, with business units having it as part of their annual commitments (balancing added value with migration costs). Moreover, we’re investing heavily in our management system with the objective to extend current ISO certifications to all entities in 2025, seeing it as an important tool to streamline our way of working, as well as a differentiator in sales and customer relations.

Metrics and targets

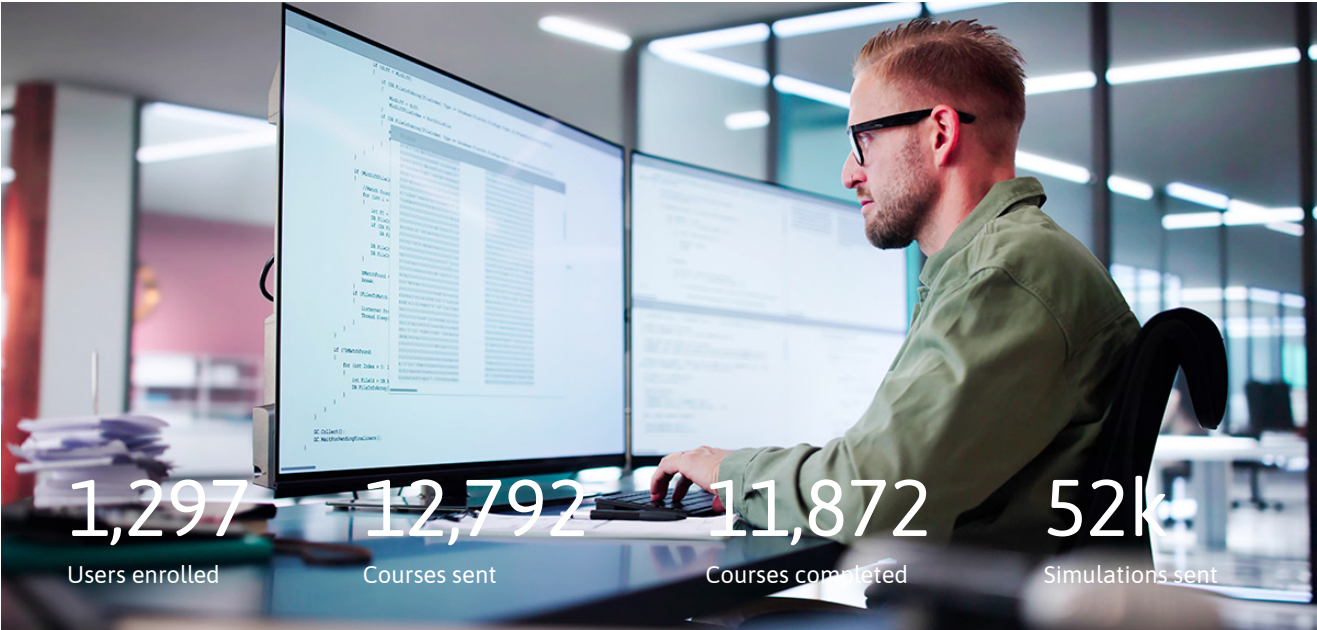
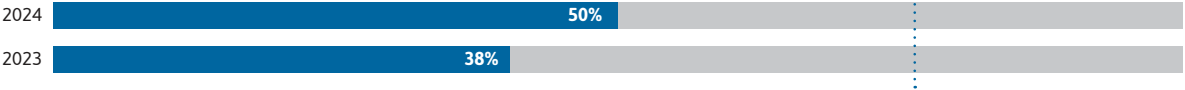
As part of our work towards achieving an ISO 27001 certification for AddSecure’s information security management system, we reviewed objectives and targets on group level.

Whether it’s a man-in-the-middle attack over Wi-Fi, a social engineering scam or something else, humans are inadvertently involved in most data breaches. In fact, 74% of incidents include some human element, such as clicking on a phishing link. At AddSecure we have therefore made employee security awareness a priority. We have introduced a training program on group level, containing micro trainings and attack simulations. Our target is to make sure that our co-workers have a high security awareness (target score 75), with 100% being onboarded on the training platform with 80% having a high engagement and activity score.

Metrics and targets

Employee security awareness
High awareness

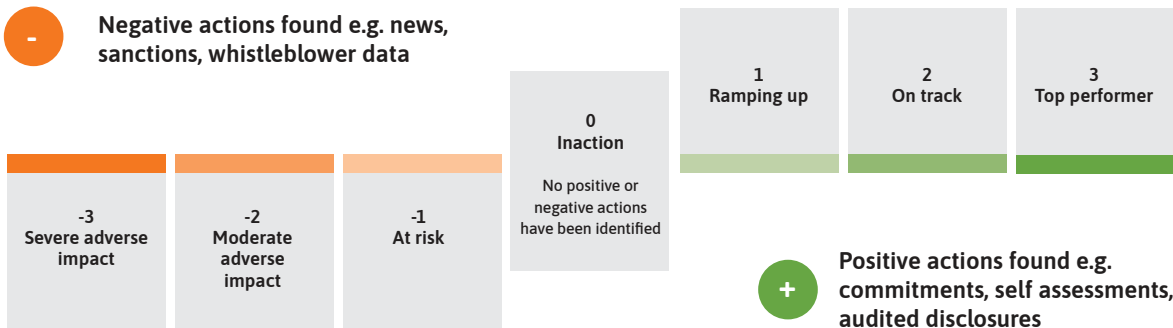
Target 2025: 75%



Workers in the value chain

Governance

AddSecure works with its supply chain to implement a shared commitment to sustainability. Our Human Rights and Labor Practices are developed to comply with legal requirements relating to enterprises' transparency and work on fundamental human rights and decent working conditions, including the Transparency Act (Åpenhetsloven) and the upcoming EU directive CS3D. We structure our work by following the six steps and supporting measures set forth in the OECD Due Diligence.



Supplier assessment: creating a shared commitment to sustainability

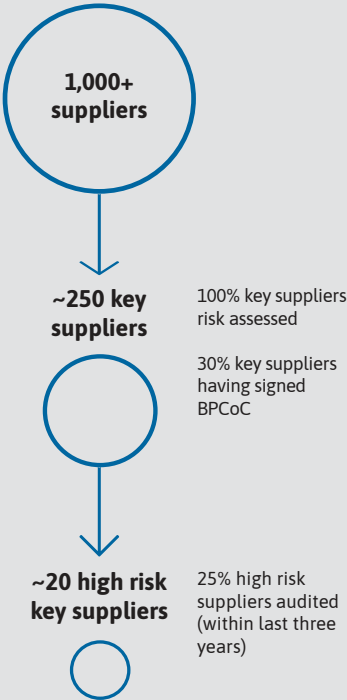
In 2024 AddSecure started the implementation of a supplier risk assessment tool to monitor and assess risks in our supply chain. By using automated data collection and AI-driven data analysis, the tool helps us evaluate and monitor suppliers, existing as well as potential. The tool constitutes an efficient instrument to collect data from suppliers, track media mentions, monitor sanction lists, and provide reports and insights on suppliers' risk profile across parameters related to environmental impact, human and labour exploitation, information security management, and regulatory violations.

The supplier risk analysis methodology uses a combination of country context and industry context to evaluate suppliers. This dual-layered approach provides a nuanced risk assessment tailored to each supplier's unique operational and geographical profile, defining risk on a scale from -3 to 3.

Risk profile

- Overall:** 22 social and 21 environmental risks identified across 176 suppliers
- Geography:** 17 social and 8 environmental risks identified across 25 sourcing countries
- Industry:** 16 social and 21 environmental risks identified across 45 supplier industries.

2024 key metrics



Strategy

Responsible business conduct and due diligence of suppliers are embedded in AddSecure’s **management system** (relevant policies, guidelines, instructions and tools).

Following the Pareto principle, **key-suppliers** are identified based on volume spend, how critical the supplier is to AddSecure’s operations, and nature of provided solution. The most important suppliers undergo a risk assessment using the group’s **supplier assessment tool**. Suppliers with a high-risk score, or prioritised for other reason, are subject for further analysis in the **Supplier management team**.

Prioritised suppliers are **audited on-site** at least once every three-year period. The audit is documented using the AddSecure audit protocol, covering topical areas such as governance, business ethics, workforce, environment and information security. Audit results are discussed within the Supplier management team. If problematic findings are made, **action plans and goals for improvements** are discussed and established with the supplier. If no satisfactory progress is made the supplier relationship is ended. When appropriate, AddSecure may provide remedial actions for identified adverse impacts.

The due diligence process, performance and actions taken are communicated through the annual sustainability statement.

Management system

- Policies:** Business Partner code of conduct, Purchasing policy.
- Guidelines:** Risk management guidelines, Whistleblowing guidelines
- Instructions:** Supplier assessment tool, Supplier audit protocol
- Resources:** Supplier management team



Business conduct

Governance

AddSecure operates a “zero tolerance” policy towards fraudulent, dishonest or deceptive behaviour, and condemns corruption in all its forms. Our Code of Conduct sets out guiding principles on how we do business, and what is expected of our employees. The Code applies to everyone working at AddSecure, whether as an employee, consultant, board member or part of the Group management. All new employees are introduced to our business principles in connection with the onboarding process. All employees receive regular training in our fair business practices and anti-corruption guidelines. We offer a whistleblowing service, available for anyone who wishes to report misconduct, serious situations or incidents concerning AddSecure. The whistleblowing service is provided by an external partner to ensure anonymity.

Strategy

AddSecure strives to achieve transparency and a high level of business ethics. Our whistleblowing service offers a possibility to alert us about suspicions of misconduct in confidence. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage. We work with our supply chain to implement a shared commitment to sustainability.

70%

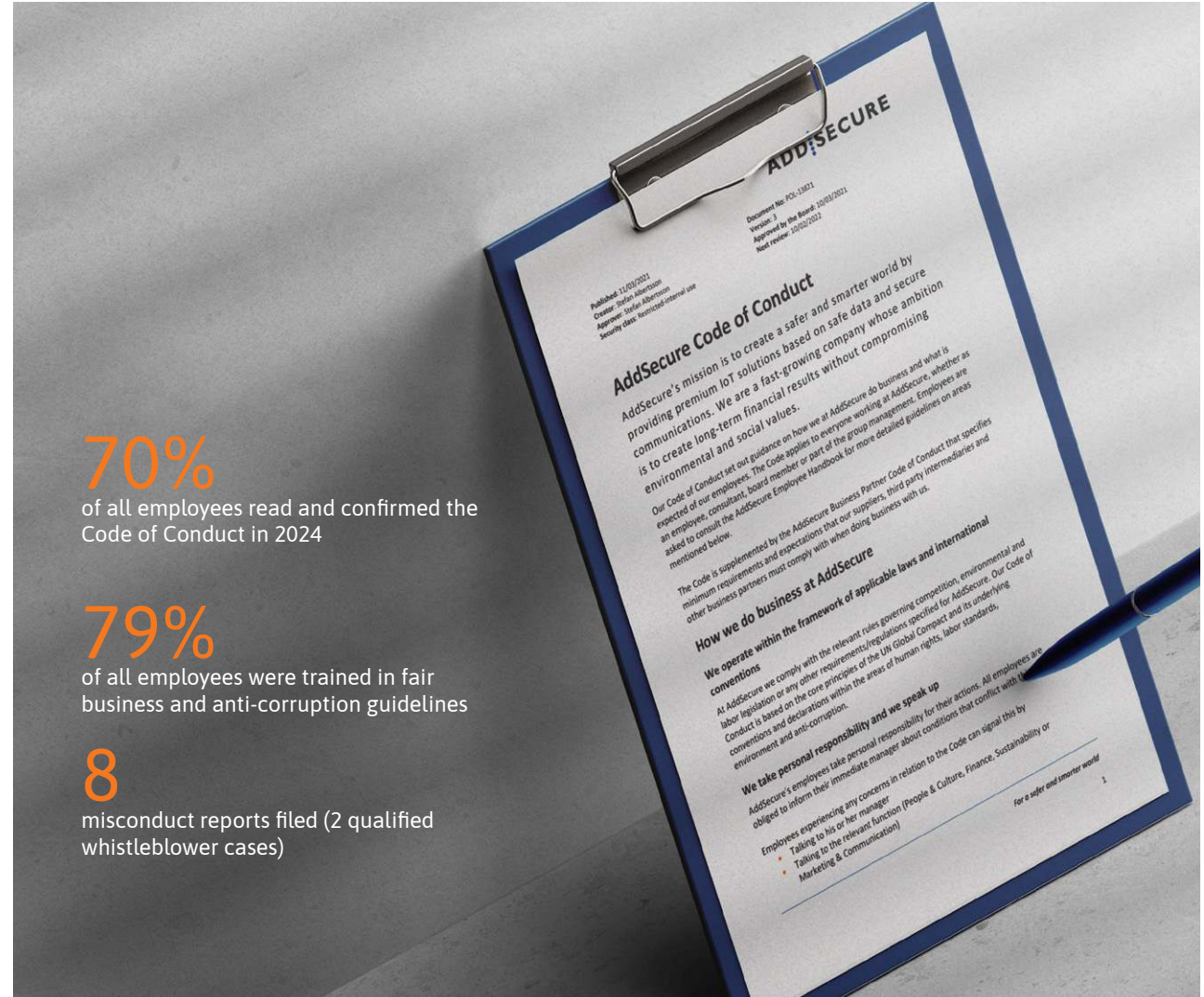
of all employees read and confirmed the Code of Conduct in 2024

79%

of all employees were trained in fair business and anti-corruption guidelines

8

misconduct reports filed (2 qualified whistleblower cases)



A hand is shown interacting with a tablet computer. The tablet screen displays a line graph with a blue line and a green shaded area. The background is dark with out-of-focus orange and yellow lights, creating a bokeh effect. The word "ADD:SECURE" is overlaid in white text, with the colon consisting of three vertical dots.

ADD:SECURE

AddSecure Group
Telefonvägen 26
126 26 Hägersten
Stockholm
Sweden